AO 106 (Rev. 04/10) Application for a Search Warrant

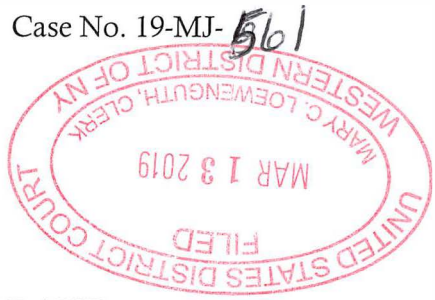
United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Email account jd.zdunich68@gmail.com, stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Case No. 19-MJ- 561



APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the Western District of New York *(identify the person or describe the property to be searched and give its location)*: Email account jd.zdunich68@gmail.com, stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B, Schedule of Items to be Seized, which attachment is incorporated by reference as if fully set forth herein, all of which are fruits, evidence and instrumentalities of a violation of Title 18, United States Code, Sections 1343 & 1030.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1343 & 1030.

The application is based on these facts: *See* attached affidavit.

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Meredith Fitzpatrick, S/A FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: March 13, 2019

Judge's signature

City and state: Rochester, New York

Hon. Jonathan W. Feldman, U.S. Magistrate Judge
Printed name and Title

19MJ561

ATTACHMENT A – GOOGLE

Property to be Searched

This warrant applies to information associated with the following email account stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

a. jd.zdunich68@gmail.com

19MJ561

ATTACHMENT B – GOOGLE

I. Information to be Produced and/or Disclosed by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. The contents of all text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;

b. All records or other information regarding the identification of the account subscriber and/or user(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All device information associated with the account to include, but not limited by, IMEI/MEID, serial number, SIM operator, cell operator, and model number;

d. All location history associated with the account. All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates, the dates and times of all location recordings, and origin of how the location recordings were obtained and estimated radius;

e. Web search history, including, but not limited to, mobile and desktop browser searches;

f. The types of service utilized;

g. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

i. Voice and/or audio activity captures;

j. Google Map location saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google Map and/or Maze services;

k. Communication including, but not limited to, audio, video, text message and/or chat delivered through the Google, Inc. service known as Google Hangouts;

l. Posts, status updates, and/or any other information including photographs and/or video for the Google, Inc. service known as Google+;

m. Photographs and/or videos that are contained and/or were uploaded in the Google, Inc. services known as Google Photos, Picasa web albums, Google+, or any other Google, Inc. service designed to store video, photographs, and/or data, including the metadata for each file;

n. Electronic files, folders, media, and/or data uploaded and/or contained on the Google, Inc. service known as Google Drive;

o. Entries created, deleted, or modified using the Google, Inc. service known as Google Keep;

p. Historical account information, including call forwarding numbers and account backup telephone number; subscriber registration information, sign-up IP address and associated time stamp, telephone connection records, billing information, stored text message content, stored voicemail content, any and all apps installed using referenced email, Google Play Store transactions, call records, and IP log information;

q. For all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, recovery email address, or telephone number, provide:

    1. Names (including subscriber names, user names, and screen names);

    2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);

    3. Local and long distance telephone connection records;

    4. Records of session times and durations and IP history log;

    5. Length of service (including start date) and types of service utilized;

    6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile

19MJ561

Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));

7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and

8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

II. Information to be Searched and Seized by the Government

1. All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

2. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and any co-conspirators, the names, addresses, and any disposition of the proceeds of the crimes under investigation, including;

3. Records relating to who created, used, or communicated with the account or identifier;

4. Records pertaining to accounts held with companies providing Internet access or remote storage of tangible items, documents, data, or storage media;

5. Records relating to ownership or use of phones including passwords, pins, and encryption keys necessary to access such devices and/or applications on devices (e.g., voicemail)

6. Records, including, but not limited to, video files, audio files, images, stored messages, recordings, books, documents, and cached web pages relating to the wire fraud scheme;

7. Records reflecting the communications with or the existence, identity, travel, or whereabouts of, any co-conspirators;

8. Any other identifying information associated with the user of the account (financial information, employment information, patterns of behavior, etc.);

9. Records of activities or usage relating to the operation or ownership of any computer hardware, software, storage media, Internet / online accounts, or data (such as usernames, passwords, telephone records, and notes).

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF EMAIL ACCOUNT: *Jd.zdunich68@gmail.com*	Case No. 19MJ561

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Meredith Fitzpatrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since June, 2017. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet-based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I make this affidavit in support of an application for a search warrant authorizing the search of an email account controlled by the Service Providers known as Google LLC (Google), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

4. The email account and the information to be searched are described in the following paragraphs and in Attachments A and B for the Service Provider. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Service Providers to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account, including contents of communications.

5. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 (wire fraud), the TARGET OFFENSE, will be found in the account *jd.zdunich68@gmail.com*.

6. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com, like the account listed in Attachment A. I have learned that opened and unopened email for subscribers, may be located on the computers owned or leased by Google. This application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.

7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

RELEVANT STATUTES

8. This investigation concerns alleged violations of 18 U.S.C. § 1343:

9. 18 U.S.C. § 1343 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme.

PROBABLE CAUSE

10. Hilliard Corporation (Hilliard) is a motion control and filtration products manufacturing company headquartered in Elmira, New York, within the Western District of New York.

11. Hilliard utilized Microsoft's Office365 product for their business email accounts. Your affiant knows that Microsoft Office 365 is a subscription of services offered by Microsoft to include email, file storage, and file sharing. OneDrive is a file hosting and synchronization service within Office365.

12. On November 19, 2018, C.V., Senior Vice President and Chief Information Officer for Hilliard, contacted the FBI Buffalo, Corning Resident Agency. C.V. alleged that two

Hilliard employees, herein referred to as VICTIM 1 and VICTIM 2, who provided their email credentials to an unknown actor as the result of a phishing email experienced unauthorized changes to their 401K accounts. VICTIM 1 had an $82,000.00 unauthorized withdrawal attempt from their 401K account and VICTIM 2 had $157,500.00 fraudulently withdrawn from their 401K account, nearly depleting it.

13. The 401K accounts for Hilliard employees were held by Chemung Canal and Trust Company (Chemung Canal), a chartered trust company headquartered in Elmira, New York.

14. In a statement to you affiant, C.V. provided the following: On November 19, 2018 Chemung Canal contacted Hilliard to report that a cyber actor impersonated two Hilliard employees to Chemung Canal and made modifications to their 401K accounts. Chemung Canal was notified of the incident because one of the Hilliard employees, VICTIM 1, called Chemung Canal stating that they received notice in the mail regarding a withdrawal from their 401K account, but they never authorized one.

15. Following the notification from Chemung Canal, Hilliard conducted an internal investigation and found that in September 2018, a Hilliard employee had their email compromised by a phishing attachment. That employee's email address was then accessed without authorization and sent the same phishing email attachment to its entire address book, which included many other Hilliard employees. The phishing email contained a .pdf attachment which, when opened, instructed the recipient to click on a View Document button to view a document sent to them with OneDrive, and provide their Office365 credentials.

16. C.V stated that Hilliard Information Technology (IT) Security staff assessed that both VICTIM 1 and VICTIM 2 had opened the phishing attachment and provided their credentials.

17. As observed by your affiant, the Office365 IP Address login history for VICTIM 1's email account showed attempted and successful logins from IP Addresses that resolve to locations outside of Elmira, NY from the period of September 11, 2018 –November 6, 2018. The Event Log history for VICTIM 2's email account showed numerous attempted logins from IP Addresses that resolve to locations outside of Elmira, NY from the period of September 13, 3018 to October 21, 2018.

18. Based on my training and experience investigating cyber-crimes, cyber actors attempt to monetize information learned from a victim's email account, and it is common for victims of email intrusions to subsequently experience unauthorized financial activity. Cyber actors accomplish this by gathering intelligence form the victim's account, such as Personally Identifiable Information (PII), where the victim holds financial accounts, and answers to security questions. Cyber actors use this information to accurately impersonate the victim to a financial entity and conduct fraudulent transactions.

19. In a statement to your affiant, K.M., Executive Vice President of Chemung Canal, provided the following: In a legitimate 401K withdrawal transaction, a customer contacts Chemung Canal requesting the withdrawal, and is then required to answer a series of identity verification questions, such as the account holder's Social Security Number. If the questions are answered correctly, Chemung Canal emails the customer a 401K withdrawal request form to complete. The customer sends the form back to Chemung Canal by fax for email, and Chemung Canal sends a confirmation letter to the customer's address on file after the withdrawal is completed.

20. K.M. further stated that an internal investigation found that in October 2018 an individual purporting to be VICTIM 2 contacted Chemung Canal and requested a withdrawal from their 401K account. The fraudulent actor correctly answered the verification questions for VICTIM 2 and requested that the 401K disbursement form be sent to the email address davidwilliams@usa.com. The fraudulent actor sent the 401K disbursement request form back via fax and requested that the funds be transferred to Zions Bank account #982187288.

21. The fraudulent actor repeated this process several times, successfully transferring $157,500.00 from VICTIM 2's 401K account to Zions Bank account #982187288 from the time period of October 4, 2018 to October 29, 2018.

22. Based on my training and experience investigating cyber-crimes, specifically 401K scams, fraudulent actors often create email accounts containing the victim's name to further bolster their false identity as the victim to the financial entity.

23. Copies of the 401K disbursement request forms sent by the cyber actor to Chemung Canal showed that on October 4, 2018, the fraudulent actor requested a $74,000.00 transfer from the 401K account of VICTIM 2 into Zions Bank account #982187288. On October 18, 2018, the fraudulent actor requested a $68,500.00 transfer from the 401K account of VICTIM 2 into Zions Bank account #982187288. On October 29, 2018, the fraudulent actor requested a $15,000.00 transfer from the 401K account of VICTIM 2 into Zions Bank account #982187288. On November 6, 2018, the fraudulent actor requested an $82,000.00 transfer from the 401K account of VICTIM 1 into Zions Bank account #579548657.

24. On March 1, 2019 your affiant received the results of a subpoena from Zions Bank for account #982187288. Records provided by Zions Bank showed the following information for the account: Account Name: John D Zdunich, Signer relationship: Sole Owner, Signer address: 2514 W Carl Cir., Taylorsville, UT 84129. The records also showed that Zdunich's utilized Zions Bank's online baking platform for account #982187288, and used the email address *jd.zdunich68@gmail.com* for his online banking account.

25. The account statements showed that the account received multiple wire transfers from Chemung Canal from the time period of October 11, 2018 and November 1, 2018.

Following the receipt of the wire transfers from Chemung Canal, Zdunich rapidly depleted the account through the use of over over thirty different cashier's checks and money orders.

26. On February 28, 2019, your affiant spoke with R.P., the Zions Bank Corporate Security Officer. R.P. provided the following in a statement to your affiant: Zions Bank conducted an investigation of account #982187288 as the account took in multiple large wire transfers and then rapidly depleted the account, which was typical of fraudulent activity. G.A., a personal banker at the Zions Bank branch where Zdunich bank, questioned Zdunich about his suspicious activity. G.A.'s notes from the interaction stated that Zdunich was uncooperative when asked about the nature of his transactions.

27. Based on my training and experience investigating cyber-crimes, specifically 401K scams, Zdunich is performing the role of a money mule. 401K schemes are often executed with a cyber actor(s) facilitating the 401K theft portion of the scam, and another individual or group facilitating the receipt and transfer of the illegally acquired funds. As such, communication is required between the two parties to provide details on when to expect the victim's funds and how to disburse them. Zdunich needs to communicate with the cyber actor(s) about how and when the money from Chemung Canal will be transferred to the intended recipient. It is reasonable to believe that such communication could occur over email, and that Erickson could have sent or received communications regarding this scam on *jd.zdunich68@gmail.com.*

28. Your affiant knows that banks typically send online banking notifications to the email on file for the customer, such as new login alerts and statement notifications. Given that Zdunich used the email account *jd.zdunich68@gmail.com* for his Zions online banking account, it is reasonable to believe that email communications from Zions Bank will be found in the email contents of *jd.zdunich68@gmail.com.*

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, where, when, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP Addresses from which users access their email account along with the time and date. By determining the physical location associated with the logged IP Addresses, investigators can understand the chronological and geographic context of the email

account access and use relating to the crimes under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the user at a particular time (e.g. location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offenses under investigation. For example, information in the email account may indicate the owner's motive an intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g. deleting communications in an effort to conceal them from law enforcement).

30. For the purposes of this Search Warrant, the Affiant has only included facts relevant to establish probable cause for this affidavit.

31. Based on my training and experience, as well as the facts previously stated, there is probable cause to believe that the email account *jd.zdunich68@gmail.com* is maintained by the account holder for Zions Bank account #982187288, who received the fraudulently transferred funds from Chemung Canal, and evidence of the TARGET OFFENSE will be contained in the email records.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

32. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

33. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

    a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

    b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

34. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

35. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.

36. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.

BACKGROUND REGARDING GOOGLE

37. Google was the service provider for the email address referenced within this affidavit. Based on my training and experience, I have learned the following about Google:

a. Google is a company that provides a variety of online services, including electronic mail ("email") access to the public. A Google subscriber can also store with Google files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an

email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

b. Google is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18,United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided. As part of its services, Google also provides its subscribers with the ability to set up email accounts;

c. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts;

d. Subscribers to Google may access their accounts on servers maintained or owned by Google from any computer connected to the Internet located anywhere in the world;

e. Any email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely;

f. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at Google, but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;

g. A Google subscriber can store files, including emails and image files, on servers maintained and/or owned by Google; and

h. Emails and image files stored on a Google server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Google server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Google servers.

i. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

BACKGROUND REGARDING GOOGLE AND COOKIES

38. According to representatives of Google, the company keeps records that can reveal Google accounts accessed from the same electronic device, such as the same computer or cellular phone, including account that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

39. A cookie is a small file maintained on a user's computer which can store data for a specific web browser session, or the cookie can be persistent so that it may be used for future web browsing sessions. The cookie can maintain data such as user preferences.

40. The following information regarding cookies was found on the Internet at URL https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (Mozilla develops the Firefox web browser):

    a. An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol.

    b. Cookies are mainly used for three purposes:

        1. Session management

           Logins, shopping carts, game scores, or anything else the server should remember.

        2. Personalization

           User preferences, themes, and other settings.

        3. Tracking

           Recording and analyzing user behavior

    c. When When receiving an HTTP request, a server can send a Set-Cookie header with the response. The cookie is usually stored by the browser, and then the cookie is sent with requests made to the same server inside a Cookie HTTP header. An expiration date or duration can be specified, after which the cookie is no longer sent. Additionally, restrictions to a specific domain and path can be set, limiting where the cookie is sent.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Service Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I in the Attachment B annexed hereto. Because the Service Providers are not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring the Service Providers to perform the search would be a burden upon the companies. If all the Service Providers were asked to do was produce all the files associated with the account, an employee can do that easily. Requiring the Service Providers to search the materials to determine what content is relevant would add to their burden. Upon receipt of the information described in Section I in the Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

42. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email account located on computer systems owned, maintained, and/or operated by Google, located at 1600 Amphitheatre Parkway, Mountain View, CA 94043 there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (Wire Fraud) and 1030 (Unauthorized Computer Access). I therefore respectfully request that the Court issue a search warrant directed to the Service Providers for the email account identified in the Attachment A for information described in the Attachment B.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order

that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Meredith Fitzpatrick, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 13 day of March, 2019

HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE